Hastings Communications and Entertainment Law Journal

Volume 17 | Number 2 Article 6

1-1-1994

Seeking Privacy in Wireless Communications: Balancing the Right of Individual Privacy with the Need for Effective Law Enforcement

Charlene L. Lu

Follow this and additional works at: https://repository.uchastings.edu/hastings_comm_ent_law_journal

 Part of the Communications Law Commons, Entertainment, Arts, and Sports Law Commons, and the Intellectual Property Law Commons

Recommended Citation

Charlene L. Lu, *Seeking Privacy in Wireless Communications: Balancing the Right of Individual Privacy with the Need for Effective Law Enforcement*, 17 Hastings Comm. & Ent. L.J. 529 (1994).
Available at: https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol17/iss2/6

This Note is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Communications and Entertainment Law Journal by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.

Seeking Privacy in Wireless Communications: Balancing the Right of Individual Privacy with the Need for Effective Law Enforcement

by
CHARLENE L. LU*

Table of Contents

* J.D. candidate 1995, University of California, Hastings College of the Law; B.S. 1990, University of California, Berkeley Haas School of Business. The author expresses grateful appreciation to Judith Tang, Kenneth Sumner, and Dennis Lee for their advice and assistance.

Introduction

Make way for the information superhighway! You will need your mobile telephone, wireless e-mail, and other wireless communication devices to travel on the technological fast lane. "Wireless communication" no longer means shouting into a crackling walkie-talkie. Today's "wireless communication" includes such sophisticated devices as cordless telephones, cellular telephones, pocket pagers, and personal communicators. These devices give the user mobility by allowing the user to send or receive messages from anywhere.

With a society as mobile as ours, is it any wonder that wireless communication devices have become so popular? In 1990 cordless telephones could be found in one out of every four households,[1] and an additional eleven million units were sold in the same year.[2] Approximately twelve million people in the United States own cellular telephones.[3] The popularity of wireless communication devices is increasing as technological innovations are making them more affordable.[4] "By the end of the decade, analysts project more than 25% of the United States population will want some type of wireless telephone service."[5]

Instead of using wires, wireless communication devices communicate over radio waves. Some wireless communication devices use microwaves or infrared waves, which are simply radio waves of a different frequency.[6] Basically, a message goes over telephone lines to a message switch which "packages" the signal for transmission and moves the message to an "uplink packet assembler/dissembler" (PAD).[7] The PAD transmits the signal up to a satellite, which sends the message to base stations on earth.[8] The base stations can broadcast the message to ninety percent of the United States, so one does

1. Robert A. Crook, *Sorry, Wrong Number, The Effect of Telephone Technology on Privacy Rights*, 26 WAKE FOREST L. REV. 669, 679 & n.140 (1991).

2. *Id.* at 679 & n.141.

3. John J. Keller & Gautam Naik, *New Wireless Phone Networks Take First Step Toward Reality*, WALL ST. J., Sept. 23, 1993, at B1.

4. Crook, *supra* note 1, at 679, 687.

5. *Id.*

6. Microwave transmissions are high frequency radio waves that transmit from point-to-point on line-of-sight paths between terrestrial antennas, usually via satellite. Robert W. Kastenmeier et. al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 722.

7. Angela Gunn, *Wireless Communications: Connecting Over the Airwaves*, PC MAG., Aug. 1993, at 359, 361.

8. *Id.*

not need to know the location of the recipient when sending a message.[9]

Although this process leaves communications vulnerable to interception, Title III of the Omnibus Safe Street and Crime Act of 1968[10] protects wireless communications as "aural acquisitions."[11] In cellular transmissions, voice signals are converted into FM radio waves, which are then beamed to local base stations clustered in cells. The radio waves are transmitted to and from switching stations within each cell. Calls are relayed between cells, constantly switching frequencies as users move from cell to cell.[12]

As the Clinton Administration proudly heralds the technology of the twenty-first century, it grapples with a growing problem of this decade: privacy in wireless communications. Since wireless communications use the airwaves, the communications are susceptible to interception. For instance, an ordinary AM/FM radio can intercept cordless telephone conversations. This Note will discuss possible solutions to this privacy problem. Two solutions proposed by the Clinton Administration are 1) the Clipper Chip, an inexpensive encryption device, which will still allow law enforcement to tap into communications, and 2) proposed legislation that bans technology that the government cannot decode. Other proposed solutions to the privacy issue consider law enforcement's need to be able to enforce court-ordered wiretaps. Among these solutions, holding manufacturers strictly liable for infringements on users' privacy appears to be the most promising.

I
Problem: Privacy

The greatest feature of wireless communications is the ability to send and receive messages from anywhere. However, this feature makes these devices susceptible to unauthorized interceptions by eavesdroppers and law enforcement officers. Cordless telephone conversations are vulnerable to being overheard not only by neighbors with cordless telephones but also by neighbors with normal AM/FM

9. *Id.*

10. Pub. L. No. 90-351, 82 Stat. 211 (1968) (codified as amended in scattered sections of 18 U.S.C.).

11. 18 U.S.C. § 2510(4) (1988).

12. Digitized cellular telephone communications are transmitted via wire to the telephone company switching office. The communications are then transmitted to a mobilized telephone switching office where the transmission is reformatted to cellular frequency format. Finally, the transmission is moved to the cell site for broadcast to base stations. The base stations broadcast the transmission to the receiver. Gunn, *supra* note 7, at 376.

radios. Similarly, cellular telephones are vulnerable to certain scanners.[13] When using a cordless or cellular telephone, the user's privacy could be violated without his or her knowledge.

It is not difficult to intercept wireless communications. A cordless telephone consists of a handset and a base unit. AM or FM radio signals transmit the communication from the handset to the base unit. From the base unit, the communication is transmitted over wire, just like a regular telephone call. The radio portions of those telephone calls (the portion transmitted from the handset to the base unit) can be intercepted with relative ease using a standard AM radio.[14]

To intercept cellular telephone calls all the eavesdropper needs is a radio capable of picking up those wavelengths. "And since most long-distance telephone calls are transmitted by microwave nowadays, they're not hard to listen to, either. Zeroing in on a particular telephone is harder but not impossible."[15] Televisions, VCRs, and scanners can easily intercept cellular communications.[16]

Interception is not only theoretically easy, it happens frequently. Just ask England's Prince Charles and Princess Diana.[17] There are countless other examples of eavesdropping on wireless communications. In 1984 shortwave radio operators intercepted President Rea-

13. A scanner is an electronic device that pinpoints and is able to intercept communications transversing along a specific band of frequency. Fred J. Meyer, Note, *Don't Touch that Dial: Radio Listening Under the Electronic Communications Privacy Act of 1986*, 63 N.Y.U. L. REV. 416, 424 & n.61 (1988).

14. Linda S. Robinson, *Wrong Number: Disconnecting the Cordless Telephone from the Right to Privacy*, 13 CRIM. JUST. J. 101, 106 (1991). *See also* State v. Delaurier, 488 A.2d 688 (R.I. 1985); State v. Howard, 679 P.2d 197 (Kan. 1984); John R. Kresse, *Privacy of Conversations Over Cordless and Cellular Telephones: Federal Protection Under the Electronic Communications Privacy Act of 1986*, 9 GEO. MASON U. L. REV. 335, 338-39 (1987).

15. David Kahn, *Scrambling for Privacy While Devices Are Being Developed that Could Lock Out Eavesdroppers, The Government Is Seeking a Set of Keys for Law-Enforcement Agencies*, NEWSDAY, July 21, 1993, at 50.

16. Timothy R. Rabel, Comment, *The Electronic Communications and Privacy Act: Discriminatory Treatment for Similar Technology, Cutting the Cord of Privacy*, 23 J. MARSHALL L. REV. 661, 674 & n.94 (1990). Interception of a conversation on a conventional telephone line is also easy. "It takes no more than a pair of alligator clips and a handset because the signal has not been converted or broken up and is moving along a single wire." Robert L. Hotz, *Change in Technology May Curtail Wiretaps; Surveillance: Agents Will Have Difficulty Isolating the One Conversation They Are Authorized to Intercept*, L.A. TIMES, Oct. 3, 1993, at A31.

17. Prince Charles' cellular telephone conversations with Camilla Parker Bowles were taped and published. Similarly, tapes were also made of Princess Diana's telephone conversations with a male friend who was using a mobile telephone. *How Three Private Phone Calls Went Public*, DAILY MAIL, May 13, 1993, at 11.

gan's secret communications aboard Air Force One.[18] In 1988 political rivals of Virginia Governor Wilder monitored his telephone conversations.[19] In June 1993 hackers intercepted telephone conversations between Secretary of State Warren Christopher's aides about United States missile attacks on Baghdad.[20]

These types of interception can be very harmful. The ability to intercept wireless communications undermines the wireless user's ability to communicate in confidence. It should not matter whether the communications relate to business data, legal strategy, or personal secrets.

> The confidentiality of an individual's communications is a basic right of our society. Eavesdropping was condemned as a nuisance even at common law, and the fourth amendment was included in the Bill of Rights to protect individuals against intrusions into their privacy. However, this right to privacy often conflicts with the government's interest in law enforcement and intelligence.[21]

As President Clinton noted recently, one of the government's primary responsibilities is to protect the public by enforcing the law.[22] Law enforcement officers sometimes eavesdrop pursuant to a court order in the name of protecting the public, but the ease of intercepting wireless communications may tempt the police to eavesdrop without a court order. For example, in *United States v. Hall*[23] a woman listening to her radio overheard suspicious conversations between two mobile car telephone users. After listening for a month, she informed the police. The police continued to listen for five weeks without obtaining a court order. The evidence collected led to the convictions of three individuals for drug trafficking.[24] In *State v. Delaurier*[25] a boy playing with his AM radio tuned into a frequency which allowed him and his mother to overhear the cordless telephone conversations of their neighbor, Delaurier. The mother called the police reporting that she had overheard a conversation regarding the sale of drugs. The police moved the radio to a nearby location and recorded conversations over several weeks—without a search warrant. These conversations led to

18. Steven M. Richman, *Voices that Go Bump in the Night: Conflicting Rights Under the Wiretap Statutes*, 11 SETON HALL LEGIS. J. 171, 171 & n.1 (1987).

19. John Eckhouse, *New Phones Keep Trade Secrets Safe Encryption Devices Thwart Eavesdroppers*, S.F. CHRON., July 9, 1993, at E1.

20. *Id.*

21. Lisa A. Wintersheimer, *Privacy Versus Law Enforcement—Can the Two Be Reconciled?*, 57 U. CIN. L. REV. 315 (1988) (citations ommitted).

22. Proclamation No. 6679, 59 Fed. Reg. 22,955 (1994).

23. 488 F.2d 193 (9th Cir. 1973).

24. *Id.*

25. 488 A.2d 688 (R.I. 1985).

arrests of Delaurier and others for drug sales, gambling, and prostitution. The police recordings were not excluded from evidence.[26]

Since *Hall* and *Delaurier* the police have encouraged neighbors who have accidently overheard crime-related conversations to monitor and tape what they overhear.[27] In *Tyler v. Berodt*[28] the Berodts' cordless telephone picked up conversations of their neighbor Tyler, who lived over four blocks away. The Berodts' overheard conversations regarding illegal activity and notified the police. The police encouraged the Berodts to continue to monitor the calls and tape record the conversations, all without a court order.[29]

II
The Current Patchwork of Solutions

The problem of unwarranted electronic surveillance by law enforcement officers and interception of communications by others did not arise with the advent of wireless communications. Even before wireless communications were invented, a patchwork of remedies or solutions addressed this problem: legislation[30] (including Title III of the Omnibus Safe Street and Crime Act of 1968 and the Electronic Communication Privacy Act of 1986), warning labels stating that the communications can be intercepted,[31] and devices scrambling communications.[32]

26. *Id.* at 694. *See also* Donald Battaglia, State v. Delaurier: *Privacy Rights and Cordless Telephones—The Fourth Amendment Is Put on Hold*, 19 J. MARSHALL L. REV. 1087, 1089-90 (1986).

27. H. W. William Caming, *The Whole World is Listening: A Quirk in Technology Makes It Unrealistic to Expect Privacy if Your Phone is Cordless*, 5 CRIM. JUST. 28, 29 (1991).

28. 877 F.2d 705 (8th Cir. 1989), *cert. denied*, 493 U.S. 1022 (1990).

29. *Tyler*, 877 F.2d at 706. The recorded conversations were suppressed at trial. Tyler then sued Berodt in a civil suit. The court granted Berodt's motion for summary judgment, finding no cause of action. *Id.* Robinson, *supra* note 14, at 101. *See also* Caming, *supra* note 27, at 29.

30. *See* 18 U.S.C. §§ 2510-2521 (1988).

31. *See, e.g.*, 47 C.F.R. § 15.236 (1984); S. REP. NO. 541, 99th Cong., 2d Sess. 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562.

32. *See, e.g.*, Jaleen Nelson, Comment, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and its Effect on Free Flow of Information and Privacy*, 41 UCLA L. REV. 1139, 1173 (1994); Samuel Rosenstein, Note, *The Electronic Communications Privacy Act of 1986 and Satellite Descramblers: Toward Preventing Statutory Obsolescence*, 76 MINN. L. REV. 1451, 1462 (1992).

A. Legislation

The cellular industry successfully pushed for a federal law making it illegal to pass on overheard conversations.[33] Unfortunately, the availability of technology and free access to radio signals have rendered the law toothless.[34] In essence, "[i]t's illegal to listen to a cellular-phone conversation, and it's about to be illegal to make or sell scanners that can tap cellular frequencies. People will do it anyway, and there's no law stopping your neighbor from listening to calls you make on your cordless phone."[35]

Congress further attempted to deal with the issue of protecting the privacy of wire and oral communications with the Electronic Communications Privacy Act of 1986 (ECPA).[36] The purpose of the ECPA was to provide a uniform basis for the conditions and circumstances under which the interception of wire and oral communications would be permitted.[37]

Prior to the ECPA, Title III of the Omnibus Crime Control and Safety Street Act of 1968 had regulated the manufacture, possession, and advertisement of electronic surveillance equipment.[38] Title III provided for a $10,000 fine and up to five years imprisonment for violation of its regulations.[39] For authorization to use a wiretap under this Act, law enforcement officers were required to state the facts in writing justifying a court order as well as to state the length of time the wiretap was to be maintained.[40]

In 1986 Congress enacted the ECPA to provide a civil remedy to "any person whose wire, oral, or electronic communication is inter-

33. Section 605 of the Communications Act of 1934 generally prohibited the interception, divulgence, and misuse of both wire and radio communications. 47 U.S.C. § 605 (1988). Section 605 provided, in pertinent part, that

> [n]o person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect or meaning thereof .... No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio.

Id.

34. *New Device Will Make Calls Private*, PLAIN DEALER, Apr. 17, 1993, at 1F. *See also* Rabel, *supra* note 16, at 672-73.

35. Dan Gillmor, *Feds' Phone Call Scrambler Lets Them Listen*, DETROIT FREE PRESS, May 6, 1993, at 1F.

36. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.) (amending Title III of the Omnibus Crime Control and Safety Street Act of 1968, *supra* note 10).

37. *Id.* (Findings).

38. Wintersheimer, *supra* note 21, at 322-23.

39. 18 U.S.C. § 2512 (1988 & Supp. V 1993).

40. *Id.* § 2516.

cepted, disclosed, or intentionally used in violation" of the Act's provisions,[41] with an exception, subject to judicial scrutiny, for law enforcement agencies if the interception is in connection with an investigation of certain offenses conducted pursuant to a court order.[42] The ECPA expanded the list of crimes in which electronic surveillance may be utilized, providing for differing penalties depending on intent and use of the interception.[43] The ECPA prohibits intentional interception of certain radio communications, including cellular mobile telephone and paging system transmissions.[44] Consequently, unintentional eavesdroppers of a protected communication may report what they hear to law enforcement.[45]

In general, the ECPA protects two types of communications against warrantless electronic surveillance: "wire communications" and "oral communications."[46] "Wire communications" are defined as communications transmitted by aid of a wire between the point of origin and the point of reception.[47] The term "wire communications" has been interpreted in *United States v. Hall* as any communication which is aided by wire at any point.[48] To be a "wire" communication the

41. *Id.* § 2520(a).

42. *Id.* § 2516. *See also* Russell S. Burnside, *The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies*, 13 RUTGERS COMPUTER & TECH. L.J. 451, 504 (1987). The requirements for a court order wiretap differs for electronically transmitted data than for voice communications—they can be based upon violation of any federal felony, rather than the limited list of crimes for voice communications. Kastenmeier et al., *supra* note 6, at 727-28. "Congress sought to ensure privacy of communications transmitted by wire and those made orally by criminalizing their interception and by conferring upon aggrieved parties a civil right of action against individuals who intercept protected communications." Samuel Rosenstein, *The Electronic Communications and Privacy Act of 1986 and Satellite Descramblers: Toward Preventing Statutory Obsolescence*, 76 MINN. L. REV. 1451, 1456 nn.24-25 (1992).

43. 18 U.S.C. § 2511(4). Generally, prohibited interceptions are punishable as a felony with penalties of a fine or five years in prison, or both. *Id.* § 2511(4)(a). For a first time offense (if not tortious, illegal, or for commercial gain), the penalty is less than one year prison or a fine, or both. *Id.* § 2511(4)(b). As noted above, offenders are also potentially subject to civil actions by those whose communications have been intercepted. *Id.* § 2520.

44. *Id.* § 2511(4)(b).

45. However, the ECPA prohibits the interception and disclosure of wire or oral communications without a court order. *Id.* § 2518.

46. *Id.* § 2510.

47. *Id.* § 2510(1). The statute also defines "electronic communications" as "any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." *Id.* § 2512(12).

48. 488 F.2d 193, 196-97 (9th Cir. 1973). *See also* Burnside, *supra* note 42, at 468. However, Kansas and Rhode Island do not agree with this interpretation. *See* Kastenmeier et al., *supra* note 6, at 724. The ECPA amendment eliminated the common car-

entire communication must be transmitted via wire.[49] Oral communications exclude all electronically transmitted communications.[50] The ECPA only protects oral communications uttered with a justifiable expectation of privacy.[51] If any portion of a communication were oral, then the entire communication would be characterized as oral.[52]

As the ECPA has been interpreted by the courts, cordless telephone users have no expectation of privacy.[53] The ECPA explicitly left cordless conversations unprotected "because communications made on some cordless telephones can be intercepted easily with readily available technologies such as an AM radio, [and therefore] it would be inappropriate to make the interception of such communication a criminal offense."[54] The ECPA left unresolved questions such as whether regular (landline) telephone calls to cordless telephones are also not protected. This is of particular concern in certain circumstances, such as when a caller is unaware that the other party is on a cordless telephone.[55]

However, cellular telephone users are protected because cellular telephones are interpreted as "wired" communications.[56] Thus, a reasonable expectation of privacy entitles cellular communications to full protection against warrantless, nonconsensual interceptions.[57] The ECPA covers communications between two cellular telephones and between a landline telephone and a cellular telephone.[58] This result seems odd. As technology advances, users must await a court decision

---

rier requirement for wire communications that existed under Title III. Wintersheimer, *supra* note 21, at 324.

49. 18 U.S.C. § 2510. *See also* Burnside, *supra* note 42, at 473. The court in Edwards v. Bardwell held that the use of a "bearcat scanner" to intercept a communication between a regular landline phone and a car radio telephone was not a violation of Title III, because a radio telephone was not wired. 632 F. Supp. 584, 589 (M.D. La. 1986), *aff'd* 808 F.2d 54 (5th Cir. 1986).

50. 18 U.S.C. § 2510(2).

51. *Id.* Cordless telephone conversations are not considered "wire communications" but are oral communications, and cordless phone users have no justifiable expectation of privacy due to the warnings in the owner's manual and on the label on the base of the phone unit. State v. Delaurier, 488 A.2d 688, 692-94 (R.I. 1985). *See also* Battaglia, *supra* note 26, at 1091; Caming, *supra* note 27, at 31.

52. *Delaurier*, 488 A.2d at 694.

53. *See id.* at 692-94. *See also* Caming, *supra* note 27, at 31; Robinson, *supra* note 14, at 107.

54. Robinson, *supra* note 14, at 107. *See also* Caming, *supra* note 27, at 31. (For criticism of the courts' interpretation of this statute see generally Robinson, *supra* note 14.)

55. Robinson, *supra* note 14, at 107. *See also* Burnside, *supra* note 42, at 504-05.

56. Rabel, *supra* note 16, at 672.

57. Caming, *supra* note 27, at 29.

58. Wintersheimer, *supra* note 21, at 333. For background on cellular phones, see Rabel, *supra* note 16, at 665-66.

on whether a particular device is technically "wired" and whether users can reasonably expect privacy. Until then, many wireless users will have to guess whether they have the right to expect privacy.

Radio waves are neither wire nor oral communications, so courts have analyzed them under the expectation of privacy test.[59] The courts usually deny Title III protection to communications over radio waves; they find that the user has no reasonable expectation of privacy.[60] Also, the ECPA amendment to Title III does not cover the radio portion of cordless telephone communications.[61]

Pagers which transmit only tonal sounds are not covered under the ECPA.[62] Voice and digital display pagers are protected under the ECPA[63] because they are a continuation of a wire communication and are covered under the Wiretap Act.[64] Voice communication is considered an aural communication—"a transfer of the human voice between and including the point of origin and point of reception,"[65] and is protected under Title III. The digital display pager is an electronic communication and is protected under "other acquisition" of a wire communication.[66]

Section 2512 of Title III outlaws the sale or manufacture of devices designed to intercept wire and oral communications.[67] In 1986 this restriction was expanded by the ECPA to include devices designed to intercept electronic communications.[68] However, the ECPA specifically provides for the lawful use of pen registers (devices that can record the numbers dialed to or from a telephone).[69] The United States Supreme Court has ruled that the use of a pen register

59. Edwards v. State Farm Ins. Co., 833 F.2d 535, 539-40 (5th Cir. 1987); Edwards v. Bardwell, 632 F. Supp. 584, 589 (M.D. La. 1986), *aff'd*, 808 F.2d 54 (5th Cir. 1986).

60. Meyer, *supra* note 13, at 431.

61. Wintersheimer, *supra* note 21, at 334.

62. *See* 18 U.S.C. § 2510(12). *See also* Wintersheimer, *supra* note 21, at 335. These pagers were never covered under Title III because there was no aural transfer of information. *See* 18 U.S.C. § 2510(18).

63. 18 U.S.C. § 2510(12). *See also* Wintersheimer, *supra* note 21, at 335.

64. *See* H.R. REP. NO. 647, 99th Cong., 2d Sess. 18, 24 (1986). *See also* Kastenmeier et al., *supra* note 6, at 730.

65. 18 U.S.C. § 2510(18). *See also* Wintersheimer, *supra* note 21, at 335.

66. 18 U.S.C. § 2510(4). The only federal case involving a pager pre-dates the ECPA. In Dorsey v. State the defendant telephoned messages to a paging company which transmitted the messages to a pocket pager via radio waves. The communication involved a drug deal. The police used a radio scanner to intercept the radio wave portion of the communication. The court ruled that Title III protection did not apply as there was no "wire" communication. 402 So.2d 1178 (Fla. 1981). *See also* Burnside, *supra* note 42, at 470.

67. 18 U.S.C. § 2512(1)(b).

68. *Id.*

69. 18 U.S.C. § 2511(2)(h)(i).

is permissible without a court order under Title III because 1) pen registers cannot obtain contents of telephone conversations,[70] and 2) there is no reasonable expectation of privacy in the telephone numbers an individual dials.[71] Furthermore, no judicial approval is necessary for government access to information generated by a pen register.[72]

The current laws attempting to deal with wireless communication and privacy are unclear, unpredictable as to how future technology would be interpreted under current law, and unable to keep up with technological advances.

B. Warnings

Presently, there are warnings in owner's manuals and on labels on the base of cordless telephones stating that the user should have no expectation of privacy. Specifically, the label states, "Privacy of communications may not be ensured when using this telephone."[73] However, hardly anyone reads the manual or the label. Members of the general public go about their daily lives under the misconception that their cordless telephone conversations are private. Part of the problem is that the label is on the base, not the handset.[74] Also, the implications of the warning are not clear to most people.

C. Scrambling Devices

Private industry has attempted to solve the privacy problem with coding devices that scramble wireless communications, similar to devices that scramble cable television signals. Cryptographic programs scramble readable data into a binary code of 0s and 1s that must be decrypted to be used again.[75] Software within the computerized device encrypts the conversation or data transmission before it is transmitted.[76] The combination of numbers which comprise the code is determined each time the user makes a telephone call.[77] The receiver will need a second encryption device to decode the communication.[78]

70. Smith v. Maryland, 442 U.S. 735, 741 (1979).
71. *Id.* at 742. *See also* Wintersheimer, *supra* note 21, at 327 n.90.
72. *Smith*, 442 U.S. at 746.
73. Caming, *supra* note 27, at 31.
74. Robinson, *supra* note 14, at 110-11.
75. John Mintz, *U.S. Moves to Ensure Its Ability to Eavesdrop; White House Selects Device for Scrambling Telephone, Fax, Computer Communications*, WASH. POST, Apr. 17, 1993, at A9.
76. Eckhouse, *supra* note 19.
77. *Id.*
78. *Id.*

This offers users privacy because with the code, the communications are just a bunch of garbled noise to an eavesdropper and would take hundreds of years to decode. The device plugs into the handset of any standard telephone, costs between $1,200 and $3,000, and is the size of an answering machine.[79] "Although computer encoding is now used in only a small amount of electronic communications, computer experts expect volume to grow rapidly as more of the nation's commerce begins to flow over data networks—especially wireless networks that are particularly subject to eavesdropping unless the information is coded."[80] Thousands of devices have been sold to major banks, oil companies, and law firms primarily for overseas calls.[81]

There is a downside to encryption. Law enforcement has complained that the technology has made it more difficult to catch drug dealers and other criminals.[82] These systems are expensive.[83] They have also become so sophisticated that they have rendered traditional wiretap technology obsolete.[84] Thus, even court authorized wiretaps cannot be carried out because of the technology. Wiretaps do not work on DES[85] because DES algorithms are published and have been modified by computer hackers to defeat wiretaps.[86]

III
The Clinton Administration's Proposals to Solve the Problem

The Clinton Administration has proposed two solutions toward resolving the conflict between the need for privacy and the need for effective law enforcement. The primary proposal is the inexpensive "Clipper Chip," a scrambler which the administration would like to make the industry standard in all communication devices. By using the Clipper Chip for government communications, those companies

79. *Id.*

80. *Way to Ensure Electronic Privacy; Administration Plans New Garbling System to Thwart Illegal Snoopers*, S.F. CHRON., Apr. 16, 1993, at A22.

81. Eckhouse, *supra* note 19.

82. Sandy Shore, *Controversy for Computer Privacy Code*, CHI. TRIB., Aug. 8, 1994, at B6.

83. Eckhouse, *supra* note 19.

84. Shore, *supra* note 82.

85. Data Encryption System (DES) is the de facto standard encryption system. It was developed twenty years ago by IBM, Inc. Robert L. Hotz, *Computer Code's Security Worries Privacy Watchdogs*, L.A. TIMES, Oct. 4, 1993, at A1.

86. *Administration's Encryption Initiative Not Welcomed by Industry, Experts Say*, Daily Rep. for Executives (BNA) No. 156, at D-23 (Aug. 16, 1993) [hereinafter *Administration's Encryption*]. *See also* Jack Robertson, *Panel Urges Clipper Delay as Crypto Plan Draws Fire*, ELECTRONIC NEWS 1993, June 7, 1993, at 1.

who want to communicate with the government must also use the Clipper Chip. This affordable scrambler allows the government to retain the "key" to decode the communications. In other words, law enforcement will still be able to "tap" into communications with a court order. The second proposed solution is the possibility of legislation that forces telephone companies to modify their equipment to keep other advances in technology from hampering law enforcement's ability to perform wiretaps.

A. Clipper Chip

1. Background

On April 16, 1993 the Clinton Administration announced the development of a new coding device, the Clipper Chip, and proposed initiatives to implement the Chip.[87] The Clipper Chip is a tiny circuit barely bigger than a beetle.[88] When the Chip is attached to a data transmitter, such as a telephone or fax machine, it uses a long string of numbers (an algorithm) to scramble the data so that it cannot be intercepted and decoded by a third party.[89] The Clipper Chip "enables a user to encrypt electronic documents before sending them to the intended recipient, but the recipient must have received the sender's secret key beforehand in order to decrypt the document."[90]

The Clipper Chip code is harder to crack than existing encoding systems.[91] It has an eighty digit binary code, called the Skipjack, instead of a fifty-six bit code used by DES.[92] The government has kept the algorithm classified, contending that because DES algorithms are published, they have become vulnerable to modifications that defeat wiretaps.[93] However, many industry experts argue that publishing the algorithm would not compromise its effectiveness.[94] Furthermore, since the algorithm is not public, there is no way to know if it is indeed

87. Christopher Drew, *Privacy Device Leaves Cops a Key*, CHI. TRIB., Apr. 17, 1993, at N1. *See also Administration's Encryption*, *supra* note 86; John Burgess, *Encryption Decision is Questioned*, WASH. POST, May 7, 1993, at F3; John Schwartz, *U.S. Data Decoding Plan Delayed Business and Legal Objections Reviewed*, WASH. POST, June 8, 1993, at A12.

88. Hotz, *supra* note 85.

89. *Administration's Encryption*, *supra* note 86.

90. Ellen Messmer, *NSA Has Public-Key Chip to Complement Clipper Chip; Uses Same Controversial Key Escrow System*, NETWORK WORLD, Apr. 26, 1993, at 5. *See also* Gillmor, *supra* note 35.

91. Drew, *supra* note 87.

92. Frank J. Murray, *Government Picks Affordable Chip to Scramble Phone Calls*, WASH. TIMES, Apr. 17, 1993, at C5.

93. *Administration's Encryption*, *supra* note 86. *See also* Robertson, *supra* note 86.

94. *Administration's Encryption*, *supra* note 86; Ellen Messmer, *Clipper Chip Targeted at Low-Speed Apps, NIST Says*, NETWORK WORLD, Aug. 9, 1993, at 16; Messmer, *supra* note 90.

sixteen million times[95] as complex as that used by chips now on the market.[96]

The most controversial aspect of the Clipper Chip is its "key" that would allow "key-holders" the ability to decode a Clipper Chip scrambled communication. Each chip has a unique serial number and "key."[97] The "key" is actually a long string of binary numbers (0s and 1s)[98] to be split in two.[99] When the manufacturer makes the devices, it will send the two keys for each unit to a database established by the Attorney General.[100] For each device the Attorney General will give one key to one official and the other key to another official. To unscramble a Clipper Chip coded communication, one must match the two coding keys held by different officials. Only under court-authorized operations could the officials bring the keys together.[101] In order for a law enforcement agency to intercept and decipher a private message encoded by the chip, it would have to obtain a warrant to tap a suspect's telephone, identify the chip's serial number from the broadcast,[102] record the encrypted message, and get two separate decoding keys to decrypt the recording.[103] The Attorney General would decide who would hold the keys.[104] Proposals of who would hold the keys included two government agencies,[105] such as the Commerce Department's National Institute of Standards and Technology (NIST) and a non-law enforcement section of the Treasury Department.[106] When legal authorization for the wiretap expires, the keys are destroyed.[107]

95. Murray, *supra* note 92.

96. Hotz, *supra* note 85 (arguing that the Clipper Chip is only twice as complex).

97. Kahn, *supra* note 15.

98. *Id.*

99. John Mintz & John Schwartz, *Chipping Away at Privacy? Encryption Device Widens Debate Over Rights of U.S. to Eavesdrop*, WASH. POST, May 30, 1993, at H1.

100. *Sophisticated Phone Scrambler Released by US for Private Use*, BOSTON GLOBE, Apr. 17, 1993, at 6 [hereinafter *Sophisticated Phone Scrambler*].

101. Drew, *supra* note 87. *See also* Mintz, *supra* note 75.

102. *See generally* Robert L. Hotz, *Demanding the Ability to Snoop; Afraid New Technology May Foil Eavesdropping Efforts, U.S. Officials Want Phone and Computer Users to Adopt the Same Privacy Code. The Government Would Hold the Only Key*, L.A. TIMES, Oct. 3, 1993, at A1.

103. Jube Shiver Jr., *Tapping Into High-Tech Talk: Device OKd to Help Feds Monitor Computer-Encoded Calls*, L.A. TIMES, Apr. 17, 1993, at D1. *See also* Mintz & Schwartz, *supra* note 99.

104. *Administration's Encryption*, *supra* note 86.

105. *Industry Criticizes "Clipper Chip"; Calls for Review of Other Systems*, Daily Rep. for Executives (BNA) No. 106, at D-27 (June 4, 1993) [hereinafter *Industry Criticizes*].

106. *Administration's Encryption*, *supra* note 86.

107. Hotz, *supra* note 102.

The Clipper Chip was invented by engineers at the National Security Agency (NSA),[108] "the super-secret eavesdropping and code-breaking agency,"[109] in conjunction with NIST.[110] NIST also developed another government sponsored encryption chip, named Capstone,[111] to encrypt computer data.[112]

The government licensed two California companies, Mykotronx and VLSI Technology, to manufacture and market[113] the Clipper Chips.[114] The license was not put out for competitive bidding.[115] NIST states that the government is working to get additional suppliers.[116]

Government officials want the Clipper Chip to replace America's current encryption standard, DES. DES was developed about twenty years ago and is generally considered to be breakable.[117] The government does not want to make the Clipper Chip the mandatory standard[118] but hopes to make it the de facto standard by two methods. The first method is to make the Clipper Chip so affordable and widespread that it would pervade telecommunications and make alternatives so expensive that few criminals could afford them.[119] The second method is to have government agencies, such as the Justice Department, military, and intelligence agencies, purchase and use the Clipper Chip in all its security telephones.[120] The Clinton Administration hopes that use by government agencies will make the Clipper Chip the de facto standard encryption device, just as the adoption of VHS over Beta videotape machines caused VHS to become the standard.[121]

108. Drew, *supra* note 87. *See also* Don Clark, *High-Tech Group Protests US Proposal on Privacy*, S.F. CHRON., May 28, 1993, at D1; Gillmor, *supra* note 35; Mintz, *supra* note 75; John Schwartz, *U.S. Data Decoding Plan Delayed Business and Legal Objections Reviewed*, WASH. POST, June 8, 1993, at A12.

109. Mintz, *supra* note 75; Mintz & Schwartz, *supra* note 99. The NSA is also known as the intelligence agency responsible for spy satellites and communications intercepts. *Sophisticated Phone Scrambler*, *supra* note 100.

110. *Administration's Encryption*, *supra* note 86; Murray, *supra* note 92; Schwartz, *supra* note 108; *Sophisticated Phone Scrambler*, *supra* note 100.

111. Gillmor, *supra* note 35.

112. Kahn, *supra* note 15.

113. Mintz, *supra* note 75.

114. *Administration's Encryption*, *supra* note 86; Drew, *supra* note 87; Shiver, *supra* note 103; *Sophisticated Phone Scrambler*, *supra* note 100.

115. Hotz, *supra* note 85.

116. *Administration's Encryption*, *supra* note 86.

117. Mintz, *supra* note 75.

118. Robertson, *supra* note 86.

119. Shiver, *supra* note 103.

120. Drew, *supra* note 87.

121. Murray, *supra* note 92.

Since only compatible telephones can receive secure communications from a telephone using a Clipper Chip,[122] many companies that do business with the government will need to buy telephones and computers with the Clipper Chip installed.[123] NIST wants to make the Clipper Chip the Federal Information Processing Standard.[124] Making the Clipper Chip the federal purchasing standard[125] makes it easier for federal government agencies to buy the Chip.[126] If the Clipper Chip becomes the standard it would be an attractive alternative to the current federal standard, DES.[127]

The Administration has already ordered nine thousand telephones equipped with the Clipper Chip from AT&T (a contract worth $8.17 million).[128] AT&T will insert the Clipper Chip into "small, box-like devices that attach to any desk or mobile phone to prevent eavesdropping."[129] The device would be the size of a small notebook and cost $1200.[130]

2. Purpose

The Clipper Chip was developed "to strike a balance between the need for privacy and the government's ability to intercept communications."[131] It was designed to "[h]elp companies protect proprietary information"[132] by preventing criminals, "terrorist[s] and industrial spies from decoding communications [made] over telephones, fax machines and computers while ensuring the government's ability to eavesdrop."[133] It would also prevent drug dealers and other criminals from making their communications immune from court ordered wiretaps.[134] The Administration sees the Clipper Chip as a means of "bring[ing] the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone com-

122. *Id.*
123. Mintz & Schwartz, *supra* note 99.
124. *Administration's Encryption*, *supra* note 86.
125. Ellen Messmer, *Clipper Chip Foes Denounce Scheme Over Cost Issues; Vendors and Users Rail Against Encryption Plan*, NETWORK WORLD, June 7, 1993, at 2.
126. *Administration's Encryption*, *supra* note 86.
127. *Id.*
128. *Id.*
129. *Sophisticated Phone Scrambler*, *supra* note 100.
130. Mintz, *supra* note 75. There is controversy that AT&T received this sole-source contract without competitive bidding. Messmer, *supra* note 125. For any other company to make the chip, it would have to assume a market outside the government. *Administration's Encryption*, *supra* note 86.
131. Shiver, *supra* note 103.
132. *Administration's Encryption*, *supra* note 86.
133. Mintz, *supra* note 75.
134. Drew, *supra* note 87.

munications while meeting the legitimate needs of law enforcement."[135]

Currently, the computer industry has systems that scramble data transfers and telephone conversations, but criminals are starting to use these systems to foil court-authorized wiretaps.[136] There are those in private industry who view the Clipper Chip as an attempt to head off independent private efforts to develop computerized encryption.[137] The government wants to discourage the use of highly capable, non-clipper encryption programs that are becoming increasingly popular, such as the RSA Data Security Inc. (RSA),[138] because the NSA cannot decode these systems.[139] Since approximately one million computers and software programs sold in this country employ RSA gear,[140] RSA believes the government is going to use its standards implementation and purchasing power to fight RSA.[141]

3. Advantages

The Clinton Administration touts the Clipper Chip as being better and more sophisticated than any other encryption device.[142] This cannot be confirmed, since the government will not reveal details for the private industry to examine.[143] The government has allowed a team of five cryptography experts to review the algorithm.[144] The team of experts gave an interim report on July 29, 1993 which stated that there is "no significant risk" of the code being broken.[145]

The Clipper Chip is supposedly so much more sophisticated than DES that it would take a powerful computer thirty-six years to crack Skipjack, the classified mathematical formula, compared to ten years to crack DES.[146] While cracking the DES code would take a Cray Supercomputer two hundred years to run through all of the possible

135. *Administration's Encryption*, *supra* note 86.
136. Drew, *supra* note 87.
137. Mintz, *supra* note 75.
138. *Id.*
139. Mintz & Schwartz, *supra* note 99.
140. Mintz, *supra* note 75.
141. *Id.*
142. *Administration's Encryption*, *supra* note 86; Drew, *supra* note 87.
143. Hotz, *supra* note 85; *Industry Criticizes*, *supra* note 105; Robertson, *supra* note 86; Winn Schwartau, *Crypto Policy and Business Privacy; The Clinton Administration's Proposed Clipper Chip Workplace Privacy*, PC WEEK, June 28, 1993, at 207.
144. *Administration's Encryption*, *supra* note 86.
145. *Id.* Note that the DES formula was made public so that independent computer experts and corporate cryptographers could test it to make sure it was secure. Hotz, *supra* note 85.
146. Messmer, *supra* note 94.

algorithm variations,[147] the Clipper Chip is sixteen million times more difficult than DES for an outsider to penetrate.[148]

Furthermore, the Clipper Chip allows law enforcement to do its job. However adequate DES may be in protecting the privacy of communications, law enforcement does not have access to the DES code keys.[149] Years ago, when AT&T controlled telephones and IBM controlled computers, the NSA had the two companies' cooperation in law enforcement.[150] Now with many little Baby Bells (BOCs) and even more computer companies, the NSA does not enjoy the cooperation from private industry it once had.[151]

Perhaps the best feature of the Clipper Chip is that it is a relatively inexpensive scrambling device. The cost of the Chip can be as little as thirty dollars per chip in the near future.[152] In lots of ten thousand or more[153] costs could eventually become as low as ten dollars per chip.[154] With such a low price, the Clipper Chip will be widely available to the general public,[155] unlike DES.

4. Opposition and Limitations

Despite these advantageous features, many oppose the adoption of the Clipper Chip. Thirty major electronic companies and trade associations sent an open letter to President Clinton stating that they "believe that there are fundamental privacy and other constitutional rights that must be taken into account."[156] Among those opposing the adoption of the Clipper Chip are Apple Computer, AT&T, Digital Equipment Corporation, IBM, Hewlett-Packard, Lotus Development Corporation, MCI Communications Corporation, Microsoft Corporation, RSA Data Security Inc., Sun Microsystems Inc., and the American Civil Liberties Union.[157] Many in the electronic industry are upset that they were not consulted and, more importantly, that their research and development investments on similar scrambling devices may be wiped out by adoption of the Clipper Chip.[158]

147. Robertson, *supra* note 86.
148. *Id.* It would take a billion years to break the Clipper Chip code. Mintz, *supra* note 75.
149. Robertson, *supra* note 86.
150. Mintz & Schwartz, *supra* note 99.
151. *Id.*
152. Murray, *supra* note 92.
153. Shiver, *supra* note 103; *Sophisticated Phone Scrambler*, *supra* note 100.
154. Murray, *supra* note 92.
155. *Id.*
156. Burgess, *supra* note 82.
157. Schwartau, *supra* note 143.
158. Drew, *supra* note 87; Murray, *supra* note 92.

Moreover, the industry is unwilling to trust the government with the keys to unlock encrypted information from the private sector.[159] They are concerned that "Big Brother" may be listening when he should not be.[160] However, it seems that adoption of the Clipper Chip may not increase potential Big Brother abuses. The government does not need a search warrant outside the United States, so it may use the Clipper Chip to monitor conversations where one or more of the users is outside the United States.[161] Currently, the private sector can protect its confidential communications with DES, which the government cannot decrypt.[162]

Some critics suspect that a code developed by the NSA could have a "'trapdoor'—an intentional flaw to make it easy for the government to gain access to encoded communications."[163] The government can counter such critics by pointing out that the Clipper Chip has a two key-keeper safeguard instead of one to guard against potential abuses. However, the critics do not trust those who hold the keys. Industry and civil libertarians advocate the use of one or more private organizations or companies to hold the keys, thereby ensuring that law enforcement does not overstep its bounds.[164] However, the key holder must have legal authority to participate in government surveillance and be constantly available.[165]

As long as other encryption systems are available, the Clipper Chip will be ineffective in aiding law enforcement. Criminals will merely use other encryption devices.[166] Since many criminals do not do business with the government, adoption of the Chip by government agencies would not force criminals to also adopt use of the Chip.[167] With other encryption techniques and the present federal DES available, why would anyone use the Clipper Chip when it is vulnerable to being unlocked?[168] Critics argue that the use of the Clipper Chip makes no sense unless such use is mandatory.[169] Even then, criminals and anyone else could get other encryption devices from overseas.

159. *Administration's Encryption*, *supra* note 86.
160. Mintz & Schwartz, *supra* note 99.
161. Clark, *supra* note 108.
162. *Administration's Encryption*, *supra* note 86.
163. *Id.*
164. *Id.*
165. *Id.*
166. Mintz & Schwartz, *supra* note 99; Shiver, *supra* note 103; Kahn, *supra* note 15.
167. Jack Robertson, *Government Close Up: Spooky Feds; Pushing Ahead with the Clipper Chip Telephone Encryption Scheme*, ELECTRONIC NEWS, Aug. 2, 1993, at 9.
168. *Id.*
169. Gillmor, *supra* note 35.

Many criminals already do so.[170] Unless it becomes the most widely used commercial encryption system and drives all other private competitors out of the business,[171] only law abiding citizens will use the Clipper Chip and be vulnerable to government eavesdropping.[172]

Furthermore, the Clipper Chip does not address the wider problem of how to make digital transmissions more accessible to wiretapping.[173] On a digital system, a conversation is broken down into a series of electronic 0s and 1s.[174] Thousands of digital conversations are transmitted over a single link.[175] Currently, wiretapping technology cannot isolate a single conversation for recording as required under the 1968 federal law.[176] The newest digital technology, to be completed by 1997, will effectively lock law enforcement agents out of many telephone calls on the West Coast.[177] Even if the Clipper Chip allowed law enforcement to tap any conversation it wished, is it worth the high cost to switch to the Clipper Chip from DES? Though the cost per chip is low, the cost to switch is great because a user must buy entirely different devices in order to use the Clipper Chip. The government is currently planning to purchase more than eight billion dollars worth of equipment for the Clipper Chip.[178] Private industry, such as banks who communicate electronically with the federal government, will have to use the Clipper Chip once the government adopts it.[179] It will be even more costly for multinational corporations because the Clipper Chip does not abide by international encryption standards.[180]

Another limitation of the Clipper Chip is that it cannot be exported. Some countries require "full disclosure of the algorithm" before importation.[181] In addition, multinational and foreign-based companies might not like the fact that United States authorities can

170. Drew, *supra* note 87.

171. *Id.*

172. Robertson, *supra* note 167.

173. Shiver, *supra* note 103.

174. Hotz, *supra* note 16.

175. Shiver, *supra* note 103.

176. *Id.*

177. Hotz, *supra* note 16.

178. *Administration's Encryption*, *supra* note 86.

179. Messmer, *supra* note 125. When Citibank switched to the Clipper Chip on its global net, it also needed newly trained personnel and additional hardware. *Id.*

180. *Id.*

181. *Administration's Encryption*, *supra* note 86.

unscramble its communications.[182] No one would want a scrambling device that the United States government can decode.[183]

This point may be moot since the government currently prevents the export of many powerful American-made encryption techniques. Clipper-embedded products would be largely barred for export under the State Department Arms Control List covering crypto products.[184] This law also covers DES. This is an unnecessary law because many other countries including Japan and Britain can export this technology.[185] The purpose of the State Department Arms Control List is to deny advanced technology with military uses to potential adversaries.[186] But what it denies is markets for producers by denying multinational firms the ability to use encryption devices in their own operations.[187] The United States software industry has been forced to develop two systems, one with DES for the domestic market and another without the encryption system for export.[188] The two systems are not interoperable.[189] The Clipper Chip is not compatible with the hardware and software which can be used internationally.[190]

Since the Chip cannot be exported, the Chip will hinder United States industries because it puts United States companies at odds with the rest of the world.[191] Currently, DES is widely used throughout the world.[192] Lotus says it has lost many foreign sales because customers demand strong software security like DES.[193] The DES demand will be met by other countries if not by the United States.[194] This jeopardizes forty to fifty percent of Hewlett-Packard's, Digital Equipment Corporation's, IBM's, SUN's, and even AT&T's business.[195]

Furthermore, the Clipper Chip may be inadequate for high-speed telecommunications equipment.[196] The Chip is unusable for computer

182. Drew, *supra* note 87.

183. *Administration's Encryption*, *supra* note 86; Mintz & Schwartz, *supra* note 99; John Mintz & John Schwartz, *Encryption Program Draws Fresh Attacks*, WASH. POST, Sept. 18, 1993, at C1.

184. *Administration's Encryption*, *supra* note 86; Robertson, *supra* note 86.

185. *Industry Criticizes*, *supra* note 105.

186. Fred W. Weingarten, *Communications Technology: New Challenges to Privacy*, 21 J. MARSHALL L. REV. 735, 752 (1988).

187. *Id.*

188. *Industry Criticizes*, *supra* note 105.

189. *Id.*

190. *Administration's Encryption*, *supra* note 86.

191. Robertson, *supra* note 86.

192. *Id.*

193. *Industry Criticizes*, *supra* note 105.

194. Robertson, *supra* note 86.

195. Robertson, *supra* note 167.

196. Messmer, *supra* note 94.

communications over packer-switched nets.[197] One of the industry's major complaints in regard to the Clipper Chip is that it lacks software application because of the classified algorithm.[198] NIST is unable to develop a version in software which does not compromise the algorithm.[199] Novell and others in the international industry coalition developed a network security model that can be implemented in both hardware and software.[200] Novell's model uses DES and RSA.[201] The Clipper Chip's hardware may make it more costly and less convenient.[202]

5. Current Status

The Clipper Chip proposal is under review by the congressionally chartered Federal Advisory Committee on Computer Privacy and Security and Commerce Department.[203] The thirteen member committee voted to delay a September 1, 1993 decision on adopting the Clipper Chip for the following reasons: 1) they needed time to consider various issues, including whether adoption would a) damage America's computer and communications trade, b) run-up costs of United States businesses, and c) violate American constitutional rights; 2) the Chip's algorithm might be compromised;[204] and 3) whether there were any side deals with AT&T making AT&T the sole supplier of the equipment to the Department of Justice.[205]

On June 4, 1993 another Commerce Department advisory committee, the Computer System Security and Privacy Advisory Board, decided that too little was known about the Chip to implement it as widely as the administration desires.[206] The Committee had not adequately investigated the Chip's economic implications and was not convinced the Chip would solve the problems for which it was designed.[207] Subsequently, NIST announced it would slow widespread adoption of the Clipper Chip.[208]

197. Messmer, *supra* note 125.
198. *Administration's Encryption*, *supra* note 86.
199. *Id.*
200. *Id.*
201. *Id.*
202. *Id.*
203. Robertson, *supra* note 167.
204. Robertson, *supra* note 86.
205. Messmer, *supra* note 125.
206. *Further Review Needed for Clipper Chip, Says Commerce Department Advisory Board*, Daily Rep. for Executives (BNA) No. 107, at D-23 (June 7, 1993) [hereinafter *Further Review Needed*].
207. *Id.*
208. Schwartz, *supra* note 108.

B. Regulate Technology So Non-Decodable Sophisticated Systems Can No Longer Be Used

The Clinton Administration is considering banning more sophisticated systems that law enforcement cannot crack.[209] But as Representative Markey (D-Mass.) pointed out, "banning encryption may be like banning privacy."[210] In addition, the ban will hinder United States companies' exports as well as put at risk research and development dollars already expended on sophisticated encryption systems.

Moreover, the FBI is separately seeking legislation to force telephone companies to modify their equipment to keep technological advances from hampering its ability to perform wiretaps.[211] In March, 1992 the FBI introduced a "legislative proposal that would require telecommunication firms to guarantee law enforcement access to its new information networks."[212] AT&T and other telephone companies opposed this proposal,[213] which was later withdrawn.[214]

France currently legislates technology so that sophisticated systems can no longer be used. France does not allow anyone to bring in encrypting devices because they interfere with monitoring.[215] Official wiretapping is widespread in France.[216] In France "wiretapping and electronic eavesdropping are illegal if used to uncover information about a person's sexual life or personal finances, but are permissible, at least under Article 368, if done for purposes of spying on a person's business or political activity."[217]

IV
What Are Our Options

In summary, there are a wide range of options to protect the privacy of wireless communication users or to give law enforcement the ability to conduct wiretaps, but none of the options seem to strike a harmonious balance between the two.

209. Messmer, *supra* note 125; Mintz & Schwartz, *supra* note 99; Murray, *supra* note 92.

210. Mintz & Schwartz, *supra* note 99.

211. Drew, *supra* note 87.

212. Mintz & Schwartz, *supra* note 99.

213. Drew, *supra* note 87.

214. Mintz & Schwartz, *supra* note 99.

215. Eckhouse, *supra* note 19.

216. Edward A. Tomlinson, *The Saga of Wiretapping in France: What It Tells Us About the French Criminal Justice System*, 53 LA. L. REV. 1091, 1092 (1993).

217. *Id.* at 1113 n.90.

A. Leave Technology Alone

A popular suggestion is to leave technology alone, allowing industry and the marketplace to develop systems to ensure privacy in wireless communication devices. However, this is merely maintaining the status quo, and it has already been shown that there is no potential solution to solve the problem of allowing limited law enforcement access to carry out authorized wiretaps while giving the public more privacy against unauthorized intrusions.

B. Give the Public Better Warning

The public should receive better warning of the vulnerability of their communications. For instance, cordless telephones should have a large warning label on the handset of the telephone, so that the consumer will actually see the warning. Another approach is to make explicit what it means not to be able to expect privacy when using the device, including the range of legal consequences. Once the public is aware of how vulnerable their communications are, consumer demand for devices that maintain privacy will increase and would give manufacturers incentive to devise appropriate solutions to the problem.

C. Change the Frequency for Cordless Telephones

Currently, cordless telephones share the same band of frequencies as that used by standard AM/FM radio receivers.[218] The FCC could change the assignment of frequencies to cordless telephones if there were capacity on the spectrum.[219] However, this assumes that cordless telephones could operate on other, higher frequencies. There is also the question of whether existing cordless telephones could take advantage of this change or whether they would be rendered useless once the change is made.

A change in frequency would protect cordless telephone conversations from being intercepted by radio listeners. However, cordless telephone conversations being intercepted by AM/FM radios is not the greatest privacy problem. Since most valuable data and sensitive communications pass over wireless communication devices other than cordless telephones everyday in this country, this situation would be unaffected by changing the frequency for cordless telephones. These communications would not be rendered any more secure or accessible to law enforcement by this proposal. Besides, the courts have already said that cordless telephone users have no expectation of privacy.

218. Caming, *supra* note 27, at 32.
219. Rabel, *supra* note 16, at 678.

Presumably all cordless telephone users are aware of this and accept the risks by continuing to use their telephones. Therefore, there is no need to go to such great lengths to ensure cordless telephone users' privacy.

D. Revamp Current Legislation: ECPA

The ECPA does not solve the problem due to the inconsistencies in applying the ECPA to different technology; in other words, cordless telephone users do not have any expectation of privacy whereas cellular telephone users do. Also, the ECPA does not keep pace with technology. For instance, the ECPA regards cordless telephones with encrypted systems as still having no expectation of privacy. Therefore, the implementation of the Clipper Chip also would not affect the status of communication devices under the ECPA. If the communication device did not have legal protection before the Clipper Chip, it will not have it with the Clipper Chip.

At the very least, the ECPA should be revamped so that communication devices with the Clipper Chip have an expectation of privacy that will be legally protected.

E. Regulate Technology

Banning more sophisticated systems that law enforcement cannot tap is not a good solution to the problem because it stifles ingenuity and hands over the business of encryption devices to foreign companies. In fact, some companies may leave the United States in order to be allowed to conduct their business of developing sophisticated encryption systems for the world market. Furthermore, those inclined to break the law may bring a sophisticated encryption device into the country from abroad illegally, and the government and law enforcement would still not have the ability to perform wiretaps. This leaves only small-time criminals and law abiding citizens vulnerable to government intrusion.

If the United States forces the disclosure of algorithms much like France and other nations, it will lead to the same uproar regarding Big Brother as we presently have under the proposed Clipper Chip. However, it would allow law enforcement access to codes other than the Clipper Chip. Still, it does not address the fact that modifications can be made to known algorithms to render them immune to wiretaps. The proposal also depends on companies and others to abide by the law and report their algorithms. Those involved in espionage and other sophisticated crimes would merely smuggle algorithms not presently known in the United States into the country.

F. Clipper Chip

The Clinton Administration's Clipper Chip will not solve the problem because it depends on becoming the de facto standard encryption device, which will not occur as long as people fear Big Brother may be listening. The Chip will not meet law enforcement's needs because it will only give law enforcement access to those who use the Clipper Chip in their communications. As we have already discussed, criminals are unlikely to use the Clipper Chip knowing that law enforcement could unscramble their communications. Criminals, as well as anyone concerned with privacy, would be more likely to use a modification of DES or a software encryption system not accessible to the government.

Aside from this, the Clipper Chip has application limitations because initially, it can only be used on low-speed, circuit-switched, telecommunications networks.[220] Thus, sophisticated communications networks would require different higher-speed algorithms to encode communications. The use of their multiple algorithms may create an interoperability issue.[221]

G. Clipper Chip and No One Has the Key

What about using the Clipper Chip but not allowing anyone to hold the key? If the Chip is inexpensive and widely available, then the Chip would virtually solve the problem of privacy in communications—assuming of course that the public does not believe that the NSA programmed in a "trap-door." The Clipper Chip would differ from DES in that the lower price would make it widely available and no one would know the algorithm. However, without a key, any efforts by law enforcement to tap communications would be locked-out.

H. Hold Manufacturers Strictly Liable

Another suggestion to ensure user privacy is to put the responsibility on the manufacturers of the wireless communication devices by making the manufacturers liable to their users for any breaches of privacy.[222] This has the advantage of giving manufacturers an incentive to devise their own inexpensive scrambling device. At present, the only incentive manufacturers have to develop scrambling devices is a slight competitive edge in the marketplace. Since most consumers are not aware of how vulnerable their wireless communications are to be-

220. Messmer, *supra* note 94.
221. *Id.*
222. Robinson, *supra* note 14, at 111.

ing intercepted, the widespread demand to justify the cost of developing an encryption system is lacking. However, the possibility of being held strictly liable may give manufacturers the added incentive to develop a low-cost encryption device that can be used on most communication devices. Now, will this device be one that law enforcement can decode? Probably not. Without legislation there is no incentive for a manufacturer to make a system susceptible to government eavesdropping. Thus, making manufacturers strictly liable would not solve the problem of balancing the needs of law enforcement with the needs of privacy, unless government reaches an agreement with manufacturers—perhaps permitting exportation of a newly developed encryption system if the government is the only one allowed to hold the key.

V
Conclusion

There is no proposal in sight that will completely solve the problem of giving law enforcement limited access to carry out authorized wiretaps while giving the public more privacy against unauthorized intrusions. As the use of wireless communications increases, the problem will only grow. America's traditions of freedom of speech and freedom from government intrusion make the prospect of any encryption device to which the government holds the key unlikely to be accepted by the American people. Similarly, Yankee ingenuity will not sit still for a ban on technology. Why not take advantage of the growing market and place the onerous task of a solution on the manufacturers of wireless communication devices? We should not only make the manufacturers strictly liable for intrusions of privacy but also make the manufacturers responsible for aiding the government in its law enforcement efforts. As unpopular as this may be, a cooperative private and public key-holding may be the only solution.